ABSTRACT

The method allows to register user in a public-key infrastructure based on credentials, including biometric data, such as data related to a fingerprint, presented to an authority (100) of the public-key infrastructure, comprising the steps of connecting a token (10), comprising a processor (2), an interface device (3) and a memory device (5), containing a private-key (51) and a public-key (52) for the user of the token (10) and a private-key (53) issued by the authority (100); reading biometric data (58) of the user, such as data derived from a fingerprint, by a biometric input device (1; 31); signing the biometric data (58) with the private-key (53) issued by the authority (100); sending a certification request, containing the public-key (52), signed biometric data (58) and additional credentials of the user, to the authority (100); verifying and registering the received data by the authority (100); storing the biometric data (58) in a database (104); returning a corresponding certificate (520) and storing the certificate (520) in the token. After registration the token is a secure element of the public-key infrastructure allowing to encrypt messages and securely sign messages, with digital signatures, on which a third party can rely on. In case of fraud biometric data taken from an unauthorised user can be stored in a database and later legally used as evidence.

(Fig. 1)